

Karate & Dance Fed Ltd - 17150545

Chief Executive Officer: Mr. J Byrne



Online Safety, Photography, Filming & Digital Communications Policy

Document Reference Number	SCL06
Title	Online Safety, Photography, Filming & Digital Communications
Policy Owner	Mr. Jake Byrne
Version	1.0
Date Written	14.09.2026
Date Ratified	September 2026
Next Review Date	September 2027

Version Control

Version	Last Modified	Modified By	Document Changes

1. Policy Statement

Karate & Dance Federation Ltd (KDF) recognises that photography, video, social media and digital communication can positively celebrate student achievement, strengthen communication with families and promote the work of KDF Karate and KDF Dance. KDF also recognises that digital technology can create safeguarding, privacy, data-protection and professional-boundary risks if it is not managed carefully.

KDF will therefore maintain clear controls over photography, filming, social-media content, digital communications, online interaction and the handling of student images. Images and communications involving children must be appropriate, necessary and consistent with the consent permissions held by KDF.

KDF uses Thrive4 as its designated system for managing relevant consent permissions and approved send-outs to families. WhatsApp is used for general operational updates and operates on an administrators-only posting basis, preventing members from using the channel as an unrestricted group discussion space.

KDF also uses an externally outsourced social media team, with Mr Aaron Hunt designated as the lead for KDF social media activity. Outsourcing operational social-media work does not transfer KDF's safeguarding, data-protection or organisational accountability to the external provider.

KDF's approach reflects its values of Kindness, Diversity, Friendship and supports the KDF Promise: Every Student, Every Session, Every Time.

2. Purpose

The purpose of this policy is to establish clear arrangements for online safety, photography, filming, social-media management, digital communications and the use of images involving KDF students.

It sets out who may capture and publish content, how consent is obtained and checked, how outsourced social-media activity is controlled, what communication channels may be

used, how students and families are protected online and how concerns involving digital technology are reported.

The policy is intended to enable KDF to use digital technology positively while maintaining safeguarding, professional-boundary and privacy standards.

3. Scope

This policy applies to directors, employees, coaches, administrators, volunteers, junior coaches, young leaders, outsourced social-media personnel and any other person acting on behalf of KDF.

Relevant sections also apply to students, parents, carers, spectators, visitors, hirers, contractors, photographers and external organisations where they photograph, film, communicate with or publish content relating to KDF students or activities.

The policy applies to social-media platforms, messaging systems, websites, email, Thrive4, WhatsApp, mobile phones, tablets, cameras, livestreaming, cloud storage and any other digital communication or content platform used in connection with KDF.

4. Legal and Safeguarding Framework

KDF will handle photographs, videos and other identifiable information in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 as amended, relevant provisions of the Data (Use and Access) Act 2025 and current Information Commissioner's Office guidance concerning children's information.

The ICO's updated 2026 guidance emphasises that children require particular protection when organisations process their personal information and that organisations must consider children's understanding, rights and best interests.

KDF will also apply its Safeguarding & Child Protection Policy, Safeguarding Adults Policy and relevant NSPCC Sport safeguarding guidance concerning photography, filming and online safety.

5. Safeguarding Principles for Digital Activity

Digital communication should never create a private or secret relationship between a staff member and a child. Communication must remain professional, transparent and connected to legitimate KDF activity.

Photography and filming must be viewed through a safeguarding lens rather than solely as marketing activity. A visually attractive image is not automatically an appropriate image to publish.

Where safeguarding and promotional interests conflict, safeguarding takes priority.

6. Designated Social Media Lead

Mr Aaron Hunt is KDF's designated lead for externally outsourced social media activity.

The Designated Social Media Lead coordinates operational social-media content with KDF management and is expected to understand KDF's consent, safeguarding, branding and communication requirements.

The role does not provide unrestricted authority to publish any image or information obtained through KDF. Content remains subject to KDF approval arrangements, consent records, safeguarding requirements and the terms of this policy.

7. Outsourced Social Media Team

KDF may contract an external team to create, schedule, edit or publish social-media content on its behalf. Outsourced personnel must operate as authorised service providers and must comply with KDF's instructions concerning children, consent, confidentiality, account security and appropriate content.

The team must not independently use KDF student images for another client, personal portfolio, commercial promotion or unrelated purpose unless a separate lawful and appropriately authorised arrangement exists.

KDF remains responsible for ensuring that outsourced arrangements include appropriate data-protection and safeguarding controls.

8. Access Provided to the Social Media Team

Access to KDF social-media accounts should be restricted to personnel who genuinely require it. Shared passwords should be avoided where platforms allow named or role-based access.

When a member of the outsourced team no longer requires access, permissions should be removed promptly.

The external team must not create additional administrators, transfer account ownership or connect third-party applications to KDF accounts without approval.

9. Content Approval and Oversight

KDF may establish routine content categories that the outsourced team can publish without seeking approval for every individual post, provided that the content remains within agreed safeguarding, consent and brand parameters.

Sensitive announcements, safeguarding matters, incidents, complaints, statements concerning individual students or staff and significant organisational announcements must not be published without appropriate KDF management approval.

The Designated Social Media Lead should escalate uncertainty rather than publish content where consent, context or suitability is unclear.

10. Thrive4 Consent System

KDF uses Thrive4 as its designated system for recording and managing relevant student and family consent and for approved communications or send-outs.

Before an identifiable student image is selected for KDF promotional or social-media use, the relevant permission should be checked against the current Thrive4 consent record where photography or publicity consent is required.

Staff must not rely solely on personal memory, assumptions about previous permission or the fact that a child has appeared in earlier content.

11. Consent Principles

Where KDF relies on consent for photography, filming or publication, consent must be meaningful, informed and capable of withdrawal.

The ICO states that valid consent should provide genuine choice, allow refusal without detriment and make withdrawal possible.

A student must not receive poorer coaching, fewer opportunities or less recognition because their parent, carer or the student themselves does not consent to public photography or filming.

12. Child and Parent Wishes

Where appropriate, KDF should consider both parental consent and the child's own wishes. A child who clearly indicates that they do not want to be photographed or filmed should not ordinarily be forced to participate in photography simply because parental consent exists.

NSPCC guidance recommends respecting the wishes of children and families and allowing consent to be declined or withdrawn.

KDF should make alternative arrangements so that a child who does not consent can continue participating normally in the underlying activity.

13. Withdrawal of Consent

Parents, carers or competent students may withdraw relevant photography or publication consent through KDF's normal communication arrangements.

KDF will update its Thrive4 records and stop using the image for future publication where consent was the basis for that use.

KDF will take reasonable steps to remove existing material from platforms under its control where appropriate, while recognising that information already lawfully published online may have been copied, downloaded or cached by third parties beyond KDF's direct control.

14. Taking Photographs and Videos

Only authorised people should take photographs or videos on behalf of KDF for official organisational purposes.

Staff should not use KDF sessions as opportunities to build personal image collections of students.

Where an authorised staff member uses a device temporarily to capture KDF content, the image should be transferred to the approved organisational process and removed from unnecessary personal storage as soon as reasonably practicable.

15. Appropriate Image Content

Images should present children positively, respectfully and in a manner consistent with the activity being promoted.

KDF should favour photographs that focus on participation, achievement, teamwork, instruction, performances and group activity rather than unnecessary close-up or body-focused imagery.

NSPCC Sport recommends considering clothing, camera angle, context and the possibility that genuine images may later be manipulated or misused, including through generative AI.

16. Prohibited Photography and Filming

Photography and filming must not take place in toilets, changing areas, intimate-care situations or any environment in which a person has a reasonable expectation of additional privacy.

Images must not be deliberately captured from sexualised, intrusive or compromising angles.

Any concern that somebody is secretly or inappropriately photographing a child in a private environment must be reported immediately through KDF safeguarding procedures and may require police involvement.

17. Student Identification

KDF should avoid unnecessarily publishing identifying information alongside images of children.

Full names, precise personal information, school details, addresses, medical information or other sensitive information should not ordinarily accompany publicly accessible images.

Where there is a legitimate reason to identify an individual student, the additional safeguarding and privacy implications must be considered before publication.

18. Group Images

Where group photographs or videos are taken, consent restrictions must still be respected.

KDF should plan how children without publication consent will be positioned or excluded from official capture without drawing unnecessary attention to them or making them feel punished.

Where an image inadvertently includes an identifiable child without appropriate permission, the content should not be published unless the issue can be resolved appropriately.

19. Performances, Gradings and Awards Events

KDF may photograph and film performances, gradings, awards ceremonies and similar events for organisational, family or promotional purposes.

Families should receive clear information about the photography arrangements and any restrictions applying to spectators.

Public or high-attendance events may require additional measures because photography is more difficult to control and images can be distributed rapidly online.

20. Parents, Carers and Spectators

KDF recognises that parents and carers may wish to photograph their own children. KDF may permit this subject to safeguarding, venue and event rules.

Parents and spectators should be reminded that images containing other children should be used responsibly and that publicly sharing identifiable images of other children may create privacy and safeguarding concerns.

The ICO notes that purely private family use may fall outside data-protection law, while public posting to an indefinite audience can create different obligations and expectations.

21. Restrictions on Spectator Photography

KDF reserves the right to prohibit or restrict spectator photography or filming where safeguarding, privacy, venue requirements or the nature of the activity make this appropriate.

A person refusing to follow a reasonable photography restriction may be asked to stop filming or leave the relevant area.

Any suspicious or covert photography should be reported immediately to the Safeguarding Lead or responsible staff member.

22. Professional Photographers and Videographers

Any professional photographer, videographer or content creator commissioned by KDF must receive a clear safeguarding brief.

The brief should identify where photography is prohibited, how children without consent will be identified, whether photographers may communicate directly with students, how images will be transferred and who owns or may retain the material.

NSPCC Sport recommends that external photographers should not have unsupervised or one-to-one access to children and that ownership, access, consent and retention expectations should be agreed in advance.

23. Social Media Content

KDF social-media content should reflect the organisation professionally and positively while protecting students from unnecessary identification or exposure.

Content may include class activity, achievements, events, organisational developments, staff recognition, promotional campaigns and educational information.

Content involving safeguarding incidents, medical matters, complaints, disciplinary issues or confidential family circumstances must not be used for social-media engagement.

24. Social Media Platforms

KDF may maintain official organisational accounts on appropriate social-media platforms. Account use must be authorised and access controlled.

Staff must not create unofficial accounts purporting to represent KDF Karate, KDF Dance or KDF Ltd without permission.

Official communication must remain distinguishable from personal staff accounts.

25. Direct Messages Through Social Media

Official account direct messages may be used for initial enquiries or routine organisational contact where appropriate, but sensitive student matters should be moved onto a more suitable approved communication route.

The outsourced social-media team must not develop private personal relationships with KDF students through direct messages.

Where a child contacts an official account with a safeguarding disclosure, the message must be preserved and escalated immediately to the KDF Safeguarding Lead.

26. WhatsApp General Updates

KDF uses WhatsApp for general updates to members and families.

KDF WhatsApp communication should operate on an administrators-only posting basis, so that ordinary members cannot post freely into the main update channel. This reduces inappropriate communication, excessive sharing of personal information and safeguarding concerns arising from uncontrolled group conversations.

WhatsApp should be used for appropriate operational information such as reminders, timetable changes, event notices and general updates rather than as KDF's primary system for confidential safeguarding or medical information.

27. WhatsApp Administration

Only authorised administrators should hold posting rights within official KDF WhatsApp update channels.

Administrators must communicate professionally and should not share private telephone numbers, personal medical details, safeguarding information or unnecessary student information through general member channels.

Membership of a WhatsApp channel must not create authority for staff or families to privately contact children outside KDF's approved safeguarding arrangements.

28. Thrive4 Send-Outs

Thrive4 should be used for relevant structured KDF send-outs and communications in accordance with the organisation's agreed administrative processes.

Where communication requires consent tracking, individualised information or a formal organisational record, Thrive4 should be preferred where its functionality is appropriate.

The use of multiple platforms should not result in contradictory messages or uncontrolled duplication of personal information.

29. Email and Administrative Communication

Email may be used for formal or individual correspondence where appropriate.

Sensitive information should only be sent to the intended recipient and staff should check recipient addresses before sending confidential material.

Group emails should be structured so that family contact details are not unnecessarily exposed to other recipients.

30. Staff Communication With Children

Staff should not routinely privately message children through personal WhatsApp, personal social media, Snapchat, disappearing-message services or other unapproved channels.

Where communication with a student is necessary, the communication should use KDF-approved systems and should be capable of appropriate adult or organisational oversight.

Communication must remain professional, relevant and appropriate to the staff member's role.

31. Communication With Parents and Carers

Routine student communications should ordinarily take place through parents, carers or appropriate KDF family communication systems, particularly for younger students.

Where older students communicate directly with KDF for legitimate reasons, professional boundaries remain unchanged.

Staff should avoid creating informal digital relationships that extend beyond the legitimate purpose of KDF activity.

32. Personal Social Media Accounts

Staff should maintain a clear distinction between personal social-media accounts and their KDF role.

They should avoid accepting or initiating private social-media relationships with current child students where this creates inappropriate familiarity or access.

Personal online activity may become relevant to KDF where it breaches confidentiality, damages safeguarding boundaries, involves discriminatory or abusive content or otherwise raises questions about suitability to work with children.

33. Mobile Phones During Sessions

Personal mobile-phone use should not distract staff from active student supervision.

Phones may be required for legitimate work purposes, attendance, music, emergencies, KDF communications or approved photography, but such use should remain proportionate.

Staff must not use personal devices to take unauthorised student photographs or videos.

34. KDF Devices

KDF-provided tablets, phones or computers should be used in accordance with organisational IT, safeguarding and data-protection requirements.

Devices containing student information should be protected by appropriate authentication and should not be left openly accessible to students, visitors or spectators.

Where devices are used for sign-in, attendance or Thrive4 administration, access to unrelated confidential information should remain restricted.

35. Storage of Photographs and Videos

Official KDF photographs and videos should be stored only for legitimate organisational purposes and within approved systems or accounts.

Images should not remain indefinitely on personal devices, unsecured memory cards or personal cloud accounts after they have been transferred for official use.

Retention should be proportionate to the purpose for which the content was collected, and obsolete or unnecessary content should be reviewed for deletion.

36. Sharing Content With the Outsourced Team

Only content reasonably required for the outsourced social-media service should be transferred to the external team.

The team should not receive unrestricted access to KDF student records or Thrive4 merely because they manage public communications. Consent verification should remain controlled through authorised KDF processes unless specific access has been lawfully and operationally approved.

Any transfer method used for student imagery should provide appropriate security.

37. Data Protection and External Providers

Where the outsourced social-media provider processes personal data on KDF's behalf, the relationship should be documented appropriately under data-protection requirements.

KDF should clarify permitted processing, confidentiality, security, deletion or return of data, subcontracting and what happens when the service ends.

The ICO emphasises particular care where organisations handle children's information or share data with third parties.

38. Account Security

Official digital accounts should use strong passwords and multi-factor authentication where available.

Passwords must not be distributed informally to staff who do not need access.

Suspected compromise, unusual login activity or unauthorised publication should be reported promptly and access credentials changed where necessary.

39. Livestreaming

Livestreaming of KDF activities should only occur where specifically authorised and where safeguarding and consent arrangements have been considered in advance.

Livestreams can create increased risk because images are transmitted immediately and control is lost once material is captured by viewers.

KDF should consider audience access, student consent, location information, camera angles and whether recording remains available after the stream ends. NSPCC guidance specifically includes livestreaming within photography and filming safeguarding arrangements.

40. Online Sessions and Video Calls

Where KDF delivers an online lesson, meeting or student activity, the same professional-boundary expectations apply as during face-to-face provision.

Platforms should be authorised and appropriate for the intended age group. Staff should avoid unnecessary one-to-one online meetings with children and should use transparent arrangements wherever reasonably practicable.

Students and families should be informed whether sessions are recorded.

41. AI, Image Manipulation and Deepfakes

KDF recognises that ordinary photographs of children may be copied and manipulated using generative AI, including for bullying, blackmail or sexualised fake imagery. Current

NSPCC guidance specifically identifies AI manipulation as a safeguarding risk when organisations publish children's images.

KDF will therefore consider whether every image genuinely needs to be published publicly and will avoid unnecessary exposure of children.

Staff must never use AI tools to sexualise, manipulate or create inappropriate representations of students or other identifiable individuals.

42. Nude or Semi-Nude Images and Sexual Content

Any incident involving nude or semi-nude imagery of a child, sexualised image manipulation, upskirting, covert recording or other child sexual imagery must be treated as a safeguarding concern.

Staff must not forward such material to colleagues or save additional copies merely to document the concern.

The Safeguarding Lead and police or other appropriate safeguarding agencies should be consulted according to the circumstances.

43. Cyberbullying and Online Harassment

Online bullying, discriminatory abuse, sexual harassment, threats or targeted harassment between KDF students may constitute a safeguarding or behaviour concern even where it occurs outside KDF premises.

Where the behaviour materially affects student welfare or participation, KDF may take proportionate safeguarding and behavioural action.

Staff should preserve factual information and avoid becoming involved in informal online arguments between families.

44. Reporting Digital Concerns

Any concern relating to inappropriate photography, online grooming, private staff-student communication, harmful content, cyberbullying, account compromise, inappropriate social-media publication or misuse of student imagery should be reported promptly.

Safeguarding concerns must be reported under KDF's Safeguarding Roles, Reporting & Responding to Concerns Policy.

Potential personal-data breaches should additionally be escalated under KDF's data-protection arrangements so that any legal notification requirements can be considered.

45. Removal and Correction of Content

Where KDF discovers that content has been published in error, contains a student without appropriate permission, discloses excessive personal information or otherwise creates a safeguarding concern, the content should be reviewed promptly and removed or corrected where appropriate.

Where content has been published by the outsourced social-media team, the Designated Social Media Lead must cooperate immediately with KDF management in removing or amending it.

Removing a post should not prevent KDF from preserving appropriate internal evidence where an incident requires investigation.

46. Training, Monitoring and Review

Relevant staff, administrators and outsourced social-media personnel should receive sufficient information about KDF's expectations concerning digital communication, photography, consent, student images and safeguarding.

KDF should periodically review account access, communication channels, Thrive4 consent arrangements, outsourced-provider access and whether official social-media activity remains consistent with this policy.

A serious digital safeguarding incident, inappropriate publication or data breach should trigger an earlier review and may result in changes to permissions, training or supplier arrangements.

47. Kindness, Diversity and Friendship

Kindness means respecting the dignity and wishes of students before capturing or sharing their image and communicating with families in a professional and considerate manner.

Diversity means ensuring KDF's digital content represents the breadth of its community positively without tokenism, stereotyping or exclusion. Friendship means using digital communication to strengthen community while maintaining appropriate professional boundaries.

These values require KDF to remember that students are people rather than marketing material. Their welfare and privacy must remain more important than engagement statistics, social-media reach or promotional value.

48. The KDF Promise

This policy supports the KDF Promise: Every Student, Every Session, Every Time. Students should be able to attend KDF knowing that participation does not automatically mean surrendering control over their image or becoming publicly identifiable online.

Digital communication should support safe, effective provision rather than creating additional risk. Where consent is absent or uncertain, KDF will adapt how content is captured or published rather than excluding the student from the activity itself.

49. Related Policies

This policy should be read alongside KDF's Safeguarding & Child Protection Policy, Safeguarding Adults Policy, Safeguarding Roles, Reporting & Responding to Concerns Policy, Allegations & Low-Level Concerns About Adults Policy, Prevent Duty, Radicalisation & Extremism Awareness Policy, Staff IT, Communications, Social Media, Mobile Devices & AI Policy, Professional Boundaries & Relationships Policy, Staff Code of Conduct & Professional Standards, Confidentiality, Data Protection, Conflicts, Leaving KDF

& Personnel Records Policy, Visitors, Spectators, Hirers & Contractors Safety Policy, Hire of Premises & Facilities Policy and relevant data-protection and privacy documentation.

These policies should be applied together where digital activity overlaps with safeguarding, professional conduct, data protection, external providers, student consent or organisational communications.

50. Policy Review

This policy will normally be reviewed annually, but an earlier review will take place following a serious online safeguarding concern, unauthorised publication of student imagery, significant data breach, introduction of a new communication platform, change to Thrive4 use, change to KDF's outsourced social-media provider or significant change to data-protection or safeguarding guidance.

KDF will keep its digital arrangements under active review because communication platforms, social-media practices and image-manipulation technology change rapidly. Staff and external providers must therefore follow current KDF instructions even where these introduce stronger controls than were previously in place.

KDF will continue to use photography, filming and digital communication positively while ensuring that safeguarding, consent, privacy and professional accountability remain central to every decision about how students are represented and contacted online.